

WHAT IS CLAIMED IS:

5

1. An apparatus for authenticating a digital signature, comprising:

10 a signature generating part encrypting a digital document by using a private key defined by a signer and digest information for checking whether the digital document has been tampered with, and generating a digital signature;

15 a signature synthesizing part creating image information by synthesizing the digital signature and a predetermined mark; and

20 an image embedding part embedding the image information created by said signature synthesizing part into an indicated position in the digital document.

20

25 2. The apparatus as claimed in claim 1, wherein said signature synthesizing part comprises an image information generating part generating pixel data for the image information including the digital signature,

30 wherein:

30 a palette, where first color information is defined for first index information and second color information is defined for other index information, is referred to;

35 the first index information is defined for pixels used for the predetermined mark; and

each of the other index information, which corresponds to each number of a number string forming

09685859 101100

the digital signature, is defined for each of other pixels.

5

3. The apparatus as claimed in claim 2,  
wherein said image information generating part  
assigns each of the other indication information  
10 corresponding to each number of the number string to  
each pixel from a beginning of the number string  
forming the digital signature while skipping the  
pixels used for the predetermined mark.

15

4. An apparatus for authenticating a  
digital signature, comprising:  
20 a signature extracting part extracting the  
digital signature from image information embedded  
into a digital document;

a digest obtaining part decrypting the  
digital signature by a public key opened by a signer  
25 and obtaining first digest information for checking  
whether the digital document has been tampered with;  
and

an authenticating part determining whether  
second digest information regenerated based on the  
30 digital document identically corresponds to the first  
digest information obtained by said digest obtaining  
part and authenticating the digital signature based  
on a result of the determination.

35

09685859 101100

5. The apparatus as claimed in claim 5, wherein said signature extracting part refers to a palette where first color information is defined for first index information and second color information is defined for other index information, and defines partial pixel data, formed by removing the first index information from pixel data forming the image information, as the digital signature, so as to generate the digital signature.

10

6. A method for authenticating a digital signature, comprising the steps of:

(a) encrypting a digital document by using a private key defined by a signer and digest information for checking whether the digital document has been tampered with, and generating a digital signature;

(b) creating image information by synthesizing the digital signature and a predetermined mark; and

(c) embedding the image information created in said step (b) into an indicated position in the digital document.

30

7. A method for authenticating a digital signature, comprising the steps of:

(a) extracting the digital signature from image information embedded into a digital document;

(b) decrypting the digital signature by a public key opened by a signer and obtaining first digest information for checking whether the digital

document has been tampered with; and

(c) determining whether second digest  
information regenerated based on the digital document  
identically corresponds to the first digest  
5 information obtained by said step (b) and  
authenticating the digital signature based on a  
result of the determination.

10

8. A computer-readable recording medium  
having a program recorded therein for causing a  
computer to authenticate a digital signature, said  
15 program comprising the codes of:

(a) encrypting a digital document by using  
a private key defined by a signer and digest  
information for checking whether the digital document  
has been tampered with, and generating a digital  
20 signature;

(b) creating image information by  
synthesizing the digital signature and a  
predetermined mark; and

(c) embedding the image information  
25 created in said step (b) into an indicated position  
in the digital document.

30

9. The computer-readable recording medium  
as claimed in claim 8, wherein said code (b) includes  
a code of (d) generating pixel data for the image  
information including the digital signature,

35

wherein:

a palette, where first color information  
is defined for first index information and second

09685859 101100

color information is defined for other index information, is referred to;

the first index information is defined for pixels used for the predetermined mark; and

5 each of the other index information, which corresponds to each number of a number string forming the digital signature, is defined for each of other pixels.

10

10. The computer-readable recording medium as claimed in claim 9, wherein said code (d)  
15 assigns each of the other indication information corresponding to each number of the number string to each pixel from a beginning of the number string forming the digital signature while skipping the pixels used for the predetermined mark.

20

11. A computer-readable recording medium  
25 having a program recorded therein for causing a computer to authenticate a digital signature, said program comprising the codes of:

(a) extracting the digital signature from image information embedded into a digital document;

30 (b) decrypting the digital signature by a public key opened by a signer and obtaining first digest information for checking whether the digital document has been tampered with; and

(c) determining whether second digest  
35 information regenerated based on the digital document identically corresponds to the first digest information obtained by said code (b) and

09685859 101100

authenticating the digital signature based on a  
result of the determination.

5

12. The computer-readable recording  
medium as claimed in claim 11, wherein said signature  
extracting part refers to a palette where first color  
10 information is defined for first index information  
and second color information is defined for other  
index information, and defines partial pixel data,  
formed by removing the first index information from  
pixel data forming the image information, as the  
15 digital signature, so as to generate the digital  
signature.

09685859 . 10.1.100